

PCT/JP 99/02510

17.06.99

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

REC'D 02 JUL 1999

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1998年10月28日

出 願 番 号

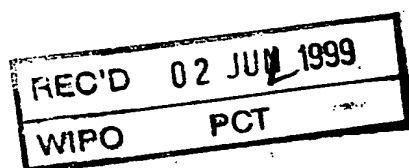
Application Number:

平成10年特許願第307658号

出 願 人

Applicant(s):

三菱マテリアル株式会社



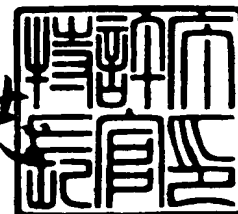
PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

Best Available Cop

1999年 4月 9日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3021090

【書類名】 特許願

【整理番号】 J75325A1

【提出日】 平成10年10月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明の名称】 暗号化装置、復号化装置、方法及びその記録媒体

【請求項の数】 10

【発明者】

    【住所又は居所】 埼玉県大宮市北袋町1丁目297番地 三菱マテリアル株式会社 総合研究所内

    【氏名】 大久保 達真

【発明者】

    【住所又は居所】 埼玉県大宮市北袋町1丁目297番地 三菱マテリアル株式会社 総合研究所内

    【氏名】 佐分利 徹

【特許出願人】

    【識別番号】 000006264

    【氏名又は名称】 三菱マテリアル株式会社

【代理人】

    【識別番号】 100064908

    【弁理士】

    【氏名又は名称】 志賀 正武

【選任した代理人】

    【識別番号】 100108578

    【弁理士】

    【氏名又は名称】 高橋 詔男

【選任した代理人】

    【識別番号】 100089037

    【弁理士】

【氏名又は名称】 渡邊 隆

【選任した代理人】

【識別番号】 100101465

【弁理士】

【氏名又は名称】 青山 正和

【選任した代理人】

【識別番号】 100094400

【弁理士】

【氏名又は名称】 鈴木 三義

【選任した代理人】

【識別番号】 100106493

【弁理士】

【氏名又は名称】 松富 豊

【選任した代理人】

【識別番号】 100107836

【弁理士】

【氏名又は名称】 西 和哉

【選任した代理人】

【識別番号】 100108394

【弁理士】

【氏名又は名称】 今村 健一

【選任した代理人】

【識別番号】 100108453

【弁理士】

【氏名又は名称】 村山 靖彦

【選任した代理人】

【識別番号】 100100077

【弁理士】

【氏名又は名称】 大場 充

【手数料の表示】

【予納台帳番号】 008707

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704954

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置、復号化装置、方法及びその記録媒体

【特許請求の範囲】

【請求項 1】 鍵暗号化部と、暗号化部とからなる暗号化装置において、  
前記鍵暗号化部は、  
共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する共通鍵  
取得部と、  
公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする共通鍵暗  
号化部と、  
前記共通鍵より共通鍵改竄検出に利用する鍵情報を作成する第 1 共通鍵改竄検  
出情報作成部とからなり、  
前記暗号化部は、  
前記共通鍵を用いて平文を暗号化し暗号文とするデータ暗号化部と、  
前記平文より第 1 データ改竄検出情報を作成する第 1 データ改竄検出情報作成  
部とからなる  
ことを特徴とする暗号化装置。

【請求項 2】 前記共通鍵暗号化部は、前記データ暗号化部により生成され  
る暗号文を共有する利用者毎に、該利用者の公開鍵を用いて前記共通鍵を暗号化  
し暗号化共通鍵を生成する  
ことを特徴とする請求項 1 記載の暗号化装置。

【請求項 3】 前記暗号化装置は、鍵復号化部をさらに備え、  
前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する  
共通鍵復号化部と、  
前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第 2  
共通鍵改竄検出情報作成部と、  
前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第 1 改竄検証部と  
からなり、  
前記鍵復号化部は、前記暗号化共通鍵を復号化し共通鍵を取得するとともに改  
竄検証し、

前記暗号化部は、前記共通鍵を用いて追加する平文をさらに暗号化することを特徴とする請求項 1 または請求項 2 に記載の暗号化装置。

【請求項 4】 請求項 1 に記載の暗号化装置によって暗号化された前記暗号化共通鍵と前記暗号文を復号化する、鍵復号化部と復号化部とからなる復号化装置において、

前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第 2 共通鍵改竄検出情報作成部と、

前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第 1 改竄検証部とからなり、

前記復号化部は、共通鍵暗号方式を利用して前記暗号文を復号化するデータ復号化部と、

前記暗号文を復号化した平文より第 2 データ改竄検出情報を作成する第 2 データ改竄検出情報作成部と、

前記第 1 データ改竄検出情報と前記第 2 データ改竄検出情報を用いて改竄検証する第 2 改竄検証部とからなる

ことを特徴とする復号化装置。

【請求項 5】 前記共通鍵復号化部は、暗号文を共有する利用者毎に対応する暗号化共通鍵のすべてを復号化し、

前記共通鍵改竄検出情報作成部は、復号化して得た共通鍵毎に前記共通鍵改竄検出情報を作成し、

前記第 1 改竄検証部は、前記鍵情報と前記共通鍵改竄検出情報から改竄検証を行なうとともに、利用者に対応する共通鍵を判定する

ことを特徴とする請求項 4 に記載の復号化装置。

【請求項 6】 請求項 1 ないし請求項 3 のいずれかに記載の暗号化装置と、請求項 4 または請求項 5 に記載の復号化装置とから構成される暗号化復号化装置。

【請求項 7】 共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得また

は生成する手順と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、

前記共通鍵より鍵情報を作成する手順と、

平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、

前記平文より第1データ改竄検出情報を作成する手順とを具備する

ことを特徴とする暗号化方法。

【請求項8】 公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、

前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、

前記暗号文を共通鍵暗号方式で復号化する手順と、

前記暗号文を復号化した平文より第2データ改竄検出情報を作成する手順と、

前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する手順とを具備する

ことを特徴とする復号化方法。

【請求項9】 共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、

前記共通鍵より鍵情報を作成する手順と、

平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、

前記平文より第1データ改竄検出情報を作成する手順とを

コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】 公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、

前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、

前記暗号文を共通鍵暗号方式で復号化する手順と、  
前記暗号文を復号化した平文より第2データ改竄検出情報を作成する手順と、  
前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する手順とを

コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報の暗号化復号化を行なう暗号化装置、復号化装置、方法及びその記録媒体に関する。

【0002】

【従来の技術】

一般に情報の伝達に際し、この情報に秘匿性が要求される場合がある。そこでさまざまな暗号化方式が考案されている。ここで従来の暗号化・著名方式を用いた暗号化装置の1例の動作フローチャートを図15に示す。この例の方式では、公開鍵暗号方式と共通鍵暗号方式を組み合わせ利用している。

まず、暗号化装置は、送信者による共通鍵の入力か、または暗号化装置側で乱数を発生させ共通鍵を生成し共通鍵を取得する（ステップS151）。

次に、公開鍵暗号方式を利用し受信者の公開鍵を用いて共通鍵を暗号化し暗号化共通鍵とする（ステップS152）。

次に共通鍵暗号化方式を利用し、平文を共通鍵を用いて暗号化し暗号文を生成する（ステップS153）。

さらにハッシュ関数を用いて平文を圧縮することでメッセージダイジェストであるMDを作成する（ステップS154）。

そして、このMDを送信者の秘密鍵で暗号化することで電子署名を付加する（ステップS155）。

送信者は、以上で生成した暗号化共通鍵と暗号文と署名をネットワーク等を介して受信者に送信する。



## 【0003】

図16に、上記暗号化・署名方式に対応する復号化方式を用いた復号化装置の動作フローチャートを示す。

復号化装置は、暗号化共通鍵と暗号文と署名を受信すると、まず受信者の秘密鍵を利用して暗号化共通鍵を復号化し共通鍵を得る（ステップS161）。

そしてこの共通鍵を用いて暗号文を復号化し平文を得る（ステップS162）。

。

次に復号化して得た平文をハッシュ関数で圧縮しメッセージダイジェストMD'を生成する（ステップS163）。

さらに受信したメッセージダイジェストMDの電子署名を送信者の公開鍵で復号化しMDを得る（ステップS164）。

次に、このMDと先のMD'を比較し、元の平文が改竄されていないかの検証を行なっている。この方式の場合、署名検証により平文への著名者を本人確認できる利点がある。

## 【0004】

次に、特開平8-156964に開示されている暗号化方式では、平文であるデータパーツが複数からなる情報を上記方式で暗号化している。図17にn個のデータパーツ（平文）からなる情報と、この情報から生成される暗号化情報の構成を示している。この場合の暗号化情報は、各データパーツに対応する暗号化共通鍵とデータパーツの暗号文とデータパーツの署名を含んでいる。一例として69バイトのデータパーツに対して付加される署名のサイズは、2329バイトである。署名のサイズには下限がありデータパーツのサイズが小さくても署名はあるサイズ以上の大きさをもつ。例えば、69バイトのデータパーツ100個から構成される情報に対し、改竄防止のために署名を付加すると、 $2329 \times 100 = 232900$ バイトの情報が付加されることになる。

## 【0005】

次に、特開平9-71388に開示されている暗号化方式では、複数のデータパーツからなる情報に対して、各データパーツのメッセージダイジェストをまとめて署名し暗号化している。図18にn個のデータパーツ（平文）からなる情報

と、この情報から生成される暗号化情報の構成を示している。

【0006】

【発明が解決しようとする課題】

複数のデータパーツからなる情報を暗号化する場合、例えば特開平 8-156964 に開示されている方式では、データのオーバーヘッドが大きくなり、暗号化情報の伝送により多くの時間がかかることや、記憶装置等の資源を多く必要とする等の問題がある。また、特開平 9-71388 に開示されている方式では、各データパーツのメッセージダイジェストをまとめて署名しているので、すべての平文がそろわないと署名の確認ができず、一部のデータパーツの参照のみ許可されているユーザがいる場合、データパーツの改竄を検証することができない点や、各データパーツを同時に変更できない等の問題がある。

【0007】

本発明は、上記の点に鑑みてなされたもので、複数のデータパーツ（平文）を含む情報を暗号化した暗号化情報のオーバーヘッドをより少なくでき、また複数のユーザで利用可能であるとともに、各データパーツの改竄検証と同時変更も可能な暗号化装置、復号化装置、方法及びその記録媒体を提供するものである。

【0008】

【課題を解決するための手段】

本発明の暗号化装置は、鍵暗号化部と、暗号化部とからなる暗号化装置において、前記鍵暗号化部は、共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する共通鍵取得部と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする共通鍵暗号化部と、前記共通鍵より共通鍵改竄検出に利用する鍵情報を作成する第 1 共通鍵改竄検出情報作成部とからなり、前記暗号化部は、前記共通鍵を用いて平文を暗号化し暗号文とするデータ暗号化部と、前記平文より第 1 データ改竄検出情報を作成する第 1 データ改竄検出情報作成部とからなることを特徴とする。

【0009】

前記共通鍵暗号化部は、前記データ暗号化部により生成される暗号文を共有する利用者毎に、該利用者の公開鍵を用いて前記共通鍵を暗号化し暗号化共通鍵を

生成することを特徴とする。

【0010】

前記暗号化装置は、鍵復号化部をさらに備え、前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第2共通鍵改竄検出情報作成部と、前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第1改竄検証部とからなり、前記鍵復号化部は、前記暗号化共通鍵を復号化し共通鍵を取得するとともに改竄検証し、前記暗号化部は、前記共通鍵を用いて追加する平文をさらに暗号化することを特徴とする。

【0011】

本発明の復号化装置は、請求項1に記載の暗号化装置によって暗号化された前記暗号化共通鍵と前記暗号文を復号化する、鍵復号化部と復号化部とからなる復号化装置において、前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第2共通鍵改竄検出情報作成部と、前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第1改竄検証部とからなり、前記復号化部は、共通鍵暗号方式を利用して前記暗号文を復号化するデータ復号化部と、前記暗号文を復号化した平文より第2データ改竄検出情報を作成する第2データ改竄検出情報作成部と、前記第1データ改竄検出情報と前記第2データ改竄検出情報を用いて改竄検証する第2改竄検証部とからなることを特徴とする。

【0012】

前記共通鍵復号化部は、暗号文を共有する利用者毎に対応する暗号化共通鍵のすべてを復号化し、前記共通鍵改竄検出情報作成部は、復号化して得た共通鍵毎に前記共通鍵改竄検出情報を作成し、前記第1改竄検証部は、前記鍵情報と前記共通鍵改竄検出情報から改竄検証を行なうとともに、利用者に対応する共通鍵を判定することを特徴とする。

【0013】

請求項6に記載の発明は、請求項1ないし請求項3のいずれかに記載の暗号化装置と、請求項4または請求項5に記載の復号化装置とから構成される暗号化復

号化装置である。

【0014】

本発明の暗号化方法は、共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、前記共通鍵より鍵情報を作成する手順と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、前記平文より第1データ改竄検出情報を作成する手順とを具備することを特徴とする。

【0015】

本発明の復号化方法は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、前記暗号文を共通鍵暗号方式で復号化する手順と、前記暗号文を復号化した平文より第2データ改竄検出情報を作成する手順と、前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する手順とを具備することを特徴とする。

【0016】

請求項8に記載の発明は、共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、前記共通鍵より鍵情報を作成する手順と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、前記平文より第1データ改竄検出情報を作成する手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体からなる。

【0017】

請求項9に記載の発明は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、前記暗号文を共通鍵暗号方式で復号化する手順と、前記暗号文を復号化した平文より第2データ改竄検出情報を作成する手順と、前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する手順とをコンピュータに実

行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体からなる。

【0018】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。

図1は、本発明の一実施形態である暗号化装置、復号化装置の構成を示すブロック図である。なお、本実施の形態では、暗号化装置と復号化装置とが一体となった暗号化復号化装置として説明する。

【0019】

本実施形態の暗号化復号化装置10は、鍵暗号化部11と、鍵復号化部12と、暗号化部13と、復号化部14とを備える。鍵暗号化部11は、共通鍵取得部15と共通鍵暗号化部16と第1共通鍵改竄検出情報作成部としての共通鍵改竄検出情報作成部17からなる。鍵復号化部12は、共通鍵復号化部18と第2共通鍵改竄検出情報作成部としての共通鍵改竄情報作成部19と第1改竄検証部としての改竄検証部20からなる。暗号化部13は、データ暗号化部21と第1データ改竄検出情報作成部としてのデータ改竄検出情報作成部22からなる。復号化部14は、データ復号化部23と第2データ改竄検出情報作成部としてのデータ改竄検出情報作成部24と第2改竄検証部としての改竄検証部25からなる。

【0020】

共通鍵取得部15は、暗号化に使用する共通鍵を取得または生成する。共通鍵の生成には、一例として乱数生成装置等を利用し生成させる。共通鍵暗号化部16は、RSA方式や楕円暗号方式等の公開鍵暗号方式を利用して共通鍵を暗号化する。暗号化に使用する公開鍵は、情報を共有するメンバーの公開鍵を使用する。例えば共有メンバーが3人の場合、3人が所持する公開鍵を用いて共通鍵を暗号化し、3つの暗号化共通鍵を作成する。共通鍵改竄検出情報作成部17は、共通鍵の正当性（①改竄されていない、②正当なユーザによって作成されている等）を検証するために利用する鍵情報を作成する。一例として、共通鍵をMD5、SHA-1等のハッシュ関数で圧縮して共通鍵のメッセージダイジェストMDを作成し、このMDに共通鍵作成者の秘密鍵を用いて署名を行なったものを鍵情報

として利用できる。署名の作成・検証には、公開鍵暗号方式の他、DSA等のデジタル署名方式等を利用してよい。

#### 【0021】

共通鍵復号化部18は、共通鍵暗号化部16により暗号化された暗号化共通鍵を公開鍵暗号方式を用いて復号化する。復号化に用いる秘密鍵は、復号化を行なうユーザの秘密鍵を用いる。共通鍵改竄検出情報作成部19は、共通鍵の正当性確認を行なうために利用する共通鍵改竄検出情報を作成する。例えば、共通鍵復号化部18で復号化された共通鍵をハッシュ関数で圧縮したメッセージダイジェストMD'を作成する。改竄検証部20は、鍵情報（一例としてMD）と共通鍵改竄検出情報作成部19で作成した共通鍵改竄検出情報（一例としてMD'）を比較検証することにより、共通鍵の正当性を確認する。共通鍵の正当性を確認するにあたり、共通鍵作成者自身の正当性確認も必要となるが、別途定められるものである。

#### 【0022】

データ暗号化部21は、データパーツ（平文）を共通鍵暗号方式を利用して暗号化し、暗号文を生成する。暗号化に使用する共通鍵は、初めて暗号化する場合には共通鍵取得部15で取得または生成された共通鍵を用い、既存の暗号化情報を利用する場合には、共通鍵復号化部18により復号化された共通鍵を用いる。データ改竄検出情報作成部22は、データパーツが改竄されていないか検証するための第1データ改竄検出情報を作成する。例えば、ハッシュ関数を用いてデータパーツを圧縮したメッセージダイジェストや、データパーツから抽出した部分情報、ID番号等を第1データ改竄検出情報として利用できる。

#### 【0023】

データ復号化部23は、共通鍵暗号方式を用いて暗号文を復号化する。復号化に用いる共通鍵は、共通鍵復号化部18により復号化された共通鍵を用いる。データ改竄検出情報作成部24は、第1データ改竄検出情報に対応しデータパーツが改竄されていないか検証するための第2データ改竄検出情報を作成する。例えば、データ復号化部23で復号化された元のデータパーツをハッシュ関数を用いて圧縮して作成したメッセージダイジェストや、データパーツから抽出した部分

情報、ID番号等を第2データ改竄検出情報として利用できる。改竄検証部25は、第1データ改竄検出情報と第2データ改竄検出情報を比較検証することにより、復号化した元のデータパーツの正当性を確認する。

## 【0024】

なお、共通鍵暗号化部16とデータ暗号化部21を、同一の装置、手段で実現してもよい。また、共通鍵復号化部18とデータ復号化部23を、同一の装置、手段で実現してもよい。また、共通鍵改竄検出情報作成部17と19、または、データ改竄検出情報作成部22と24を、同一の装置、手段で実現してもよい。同様に、共通鍵改竄検出情報作成部17と19及びデータ改竄検出情報作成部22と24のすべてを、同一の装置、手段で実現してもよい。また、改竄検証部20と改竄検証部25を、同一の装置、手段で実現してもよい。また、本実施の形態の暗号化復号化装置を、単一の装置としてではなく、各部が独立した装置、手段として実現し利用してもよい。なお、請求項1および請求項2に記載の暗号化装置は、鍵暗号化部11と暗号化部13とから構成できる。また、請求項3に記載の暗号化装置は、鍵暗号化部11と暗号化部13と鍵復号化部12とから構成できる。請求項4および請求項5に記載の復号化装置は、鍵復号化部12と復号化部14とから構成できる。

## 【0025】

図2に、本実施形態の暗号化復号化装置10の一利用形態を示す。

本利用形態では、ネットワークに接続可能なサーバや他端末装置等からなる情報保管装置30と、暗号化復号化装置10を備える端末装置31とがネットワークを介して接続されている。情報保管装置30は、ハードディスク、光磁気ディスク等の不揮発性の記録装置を備え、暗号化情報として、暗号文、データ改竄検出情報、暗号化共通鍵、鍵情報および関連情報を保存可能とする。また、端末装置31には、周辺機器として入力装置、表示装置等（いずれも図示せず）が接続されるものとする。ここで、入力装置とはキーボード、マウス等の入力デバイスのことをいう。表示装置とはCRT（Cathode Ray Tube）や液晶表示装置等のことをいう。なお、暗号化情報をローカルな端末装置31に保管し、スタンドアローンで利用してもよい。

【0026】

次に、このように構成された利用形態における本実施形態の暗号化復号化装置 10 の動作について説明する。

まず、最初のデータパーツを暗号化する際の暗号化復号化装置 10 の動作を図 3 に示す動作フローチャートを参照して説明する。なお、下記の説明における動作手順は、本実施形態の動作の一例であり、その処理の順序は固定されるものではなく他の順序で実施されてもよい。

【0027】

始めに、共通鍵取得部 15 が、暗号化復号化装置 10 の外部からの入力により共通鍵を取得するかまたは共通鍵の生成を行なう（ステップ S301）。

【0028】

それから共通鍵暗号化部 16 は、ネットワークを介して予め取得している利用者の公開鍵を利用して共通鍵を暗号化した暗号化共通鍵を生成する（ステップ S302）。

【0029】

さらに、共通鍵改竄検出情報作成部 17 は、共通鍵作成者の秘密鍵等の共通鍵作成者に関する情報を共通鍵改竄検出情報としての鍵情報として作成する（ステップ S303）。

【0030】

データ暗号化部 21 はデータパーツ 1（平文）を暗号化し暗号文 1 を生成する（ステップ S304）。

【0031】

さらに、データ改竄検出情報作成部 22 は、データパーツ 1 からデータパーツ 1 に関する情報であるデータ改竄検出情報 1 を作成する（ステップ S305）。

なお、データパーツが  $n$  個からなる場合、ステップ S304 からステップ S305 の処理を  $n$  回繰り返す。

【0032】

そして暗号文 1、2、…、 $n$ 、データ改竄検出情報 1、2、…、 $n$ 、鍵情報、暗号化共通鍵の組を暗号化情報として情報保管装置 30 へ送信する（ステップ S



306)。

【0033】

なお、上記説明は利用者が1人で、使用する暗号化共通鍵が1種類の場合である。暗号化情報を共有する利用者が複数（例えばm人）である場合は、ステップS302で、各利用者毎の公開鍵を用いてm種の暗号化共通鍵を生成させる。すなわち、利用者毎に対応する暗号化共通鍵が生成されることになる。

図4に、暗号化前の情報の構成と、暗号化された暗号化情報の構成を示す。ここでは、暗号化前のデータパーツ1、2、…、nから、暗号化情報として、暗号文1、2、…、nとデータ改竄検出情報1、2、…、nと暗号化共通鍵1、2、…、mと鍵情報が作成されることを示している。

【0034】

次に、複数（n個）のデータパーツの暗号文を含む暗号化情報を復号化する際の暗号化復号化装置10の動作を図5の動作フローチャートを参照して説明する。

なおこの処理は、暗号化共通鍵を作成する際に用いた公開鍵と対をなす秘密鍵を所有する者が行なえるものである。

【0035】

まず、暗号化復号化装置10は情報保管装置30に記憶されている暗号化情報を取得する（ステップS501）。なお、暗号化情報に含まれる暗号化共通鍵は、ユーザ名やユーザID等により対応づけられ、利用者に対応した暗号化共通鍵が情報保管装置30から暗号化復号化装置10に送られるものとする。

【0036】

そして共通鍵復号化部18は、利用者の秘密鍵を用いて暗号化共通鍵を復号化し共通鍵を得る（ステップS502）。ここで利用者の秘密鍵は、予め入力されているものとする。

【0037】

次に、共通鍵改竄検出情報作成部19は、ステップS502で得た共通鍵から共通鍵改竄検出情報を作成する（ステップS503）。

【0038】

そして改竄検証部20は、取得した鍵情報と共通鍵改竄検出情報を比較検証し鍵作成者の正当性を検証する（ステップS504）。この場合、2つの情報が一致することで鍵作成者の正当性を判断できる。

【0039】

ステップS504で、鍵作成者が正当であると判断された場合、n個の暗号文とn個のデータ改竄検出情報の組を順に以下の処理を行なう。

まず、データ復号化部23は暗号文を共通鍵を用いて復号化する（ステップS505）。

【0040】

そして、データ改竄検出情報作成部24は、復号化したデータパーツを用いてデータ改竄検出情報を作成する（ステップS506）。なお、ここで作成したデータ改竄検出情報を第1データ改竄検出情報と呼び、暗号化情報として保持されているデータ改竄検出情報を第2データ改竄検出情報と呼ぶことにする。

【0041】

次に改竄検証部25は、作成された第1データ改竄検出情報と暗号化情報の一部である第2データ改竄検出情報を比較し改竄が行われていないか検証する（ステップS507）。2つの情報が一致することで改竄が行われていないことが検証される。

【0042】

ステップS507で、改竄がないと判断されれば復号化したデータパーツ（平文）を出力する（ステップS508）。

【0043】

なお、以上の説明では、ユーザ名やユーザID等と暗号化共通鍵を対応づけることで、鍵復号化部12が利用者に対応する暗号化共通鍵のみを用いるようにしている。複数の暗号化共通鍵がある（すなわち、暗号化情報を共有する利用者が複数存在する）場合、利用者に対応する暗号化共通鍵を得るその他の方法として、上記ステップS502～S504を以下のようにする。まず、ステップS502においてすべての暗号化共通鍵を復号化する。ステップS502で複数の暗号化共通鍵を復号化した場合、正式でないものも含めて複数の共通鍵が生成される

。ステップ S503 では、ステップ S502 で生成されたすべての共通鍵に対し共通鍵改竄検出情報を作成する。次に、ステップ S504 で、各共通鍵改竄検出情報と鍵情報とを比較検証する。すべての組み合わせが異なるとき改竄が行われていることがわかり、一致するものがあれば対応する共通鍵が正式の共通鍵であることがわかる。

#### 【0044】

次に、上述した、データパーツ 1、2、…、n から暗号化情報を作成し情報保管装置 30 に転送した段階から、ここではさらに上記の暗号化情報に情報を追加する際の暗号化復号化装置 10 の動作を図 6 に示す動作フローチャートを参照して説明する。

#### 【0045】

まず、暗号化情報が保管されている情報保管装置 30 から暗号化共通鍵と鍵情報を取得する（ステップ S601）。なお、暗号化情報に含まれる暗号化共通鍵は、ユーザ名やユーザ ID 等により対応づけられ、利用者に対応した暗号化共通鍵が情報保管装置 30 から暗号化復号化装置 10 に送られるものとする。

#### 【0046】

そして、共通鍵復号化部 18 は、利用者の秘密鍵を用いて利用者に対応する暗号化共通鍵を復号化する（ステップ S602）。ここで利用者の秘密鍵は、予め入力されているものとする。

#### 【0047】

次に、共通鍵改竄検出情報作成部 19 は、ステップ S602 で得た共通鍵から共通鍵改竄検出情報を作成する（ステップ S603）。

#### 【0048】

改竄検証部 20 は、先の鍵情報と共通鍵改竄検出情報が一致するか比較検証し、鍵作成者の正当性を検証する（ステップ S604）。この場合、2つの情報が一致することで鍵作成者の正当性を判断できる。

#### 【0049】

ステップ S604 で、鍵作成者が正当であると判断された場合、データ暗号化部 21 は追加するデータパーツ n+1 を暗号化し暗号文 n+1 を生成する（ステ

ップS605)。

【0050】

さらにデータ改竄検出情報作成部22はデータパーツ $n+1$ から改竄検出情報 $n+1$ を作成する(ステップS606)。

なお、追加するデータパーツが $L$ 個からなる場合、ステップS605からステップS606の処理を $L$ 回繰り返す。

【0051】

そして暗号文 $n+1$ 、 $n+2$ 、…、 $n+L$ と改竄検出情報 $n+1$ 、 $n+2$ 、…、 $n+L$ を情報保管装置30に転送し暗号化情報として追加保管する(ステップS607)。

【0052】

なお、以上の説明では、ユーザ名やユーザID等と暗号化共通鍵を対応づけることで、鍵復号化部12が利用者に対応する暗号化共通鍵のみを用いるようにしている。複数の暗号化共通鍵がある(すなわち、暗号化情報を共有する利用者が複数存在する)場合、利用者に対応する暗号化共通鍵を得るその他の方法として、上記ステップS602～S604を以下のようにする。まず、ステップS602においてすべての暗号化共通鍵を復号化する。ステップS602で複数の暗号化共通鍵を復号化した場合、正式でないものも含めて複数の共通鍵が生成される。ステップS603では、ステップS602で生成されたすべての共通鍵に対し共通鍵改竄検出情報を作成する。次に、ステップS604で、各共通鍵改竄検出情報と鍵情報とを比較検証する。すべての組み合わせが異なるとき改竄が行われていることがわかり、一致するものがあれば対応する共通鍵が正式の共通鍵であることがわかる。

図7に、暗号化情報の追加前の構成と、追加後の構成を示す。ここでは、暗号化情報として、暗号文 $n+1$ 、 $n+2$ 、…、 $n+L$ とデータ改竄検出情報 $n+1$ 、 $n+2$ 、…、 $n+L$ がもとの暗号化情報に追加されていることを示している。

【0053】

次に、情報保管装置30に記憶されている暗号化情報を共有しているチームに、共有メンバーを追加する際の暗号化復号化装置10の動作を図8に示す動作フ

ローチャートを参照して説明する。ここでは、共有メンバーA、Bが所属しているチームに、共有メンバーBが、新しい共有メンバーとして共有メンバーCを追加する場合を説明する。

【0054】

まず、共有メンバーBの操作により、暗号化復号化装置10は情報保管装置30にアクセスし、鍵情報と共有メンバーBに対応する暗号化共通鍵Bを取得する（ステップS801）。

【0055】

共通鍵復号化部18は、受信者である共有メンバーBの秘密鍵を用いて暗号化共通鍵Bを復号化し、共通鍵を得る（ステップS802）。

【0056】

共通鍵改竄検出情報作成部19は共通鍵から共通鍵改竄検出情報を作成する（ステップS803）。

【0057】

そして改竄検証部20は、取得した鍵情報と共通鍵改竄検出情報を比較検証し鍵作成者の正当性を確認する（ステップS804）。この場合、2つの情報が一致することで改竄が行われていないことが検証される。

【0058】

ステップS804で、鍵作成者の正当性が確認されると、共通鍵暗号化部16は共有メンバーとして追加する共有メンバーCの公開鍵を用いて共通鍵を暗号化し、暗号化共通鍵Cを生成する（ステップS805）。

【0059】

鍵暗号化部12は生成された暗号化共通鍵Cを情報保管装置30へ転送する（ステップS806）。

【0060】

こうして、情報保管装置30には3人の共有メンバーに対応する暗号化共通鍵A、B、Cが保管されることになり、以後、追加された共有メンバーCは、チームの暗号化情報に対する参照・変更等を行なえるようになる。

図9に、共有メンバーCの追加前の暗号化情報の構成と、追加後の構成を示す

。ここでは、暗号化情報として、あらたな共有メンバーである共有メンバーC用の暗号化共通鍵Cがもとの暗号化情報に追加されていることを示している。

【0061】

次に、共有メンバーを削除する際の暗号化復号化装置10の動作を図10に示す動作フローチャートを参照して説明する。ここでは、共有メンバーA、B、Cが所属しているチームにおいて、共有メンバーBが共有メンバーAを削除する場合を説明する。

【0062】

暗号化復号化装置10は、共有メンバーBの入力操作による共有メンバーAを削除するための削除命令を取得する（ステップS101）。

【0063】

データ改竄検出情報作成部22は、共有メンバーAの削除命令に対応するデータ改竄検出情報を作成する（ステップS102）。

【0064】

次に、暗号化復号化装置10は、共有メンバーの削除命令と、削除命令を出した本人を識別する識別情報となるデータ改竄検出情報の組からなる削除情報を情報保管装置30に転送する（ステップS103）。

【0065】

なお、情報保管装置30は、削除命令を出した本人を識別する機能を持ち、削除命令に応じた暗号化共通鍵を削除できるものとする。また、ここで用いるデータ改竄検出情報として、共有メンバーAの削除命令に対する共有メンバーBの電子署名を用いてもよい。また、削除命令を出した本人を識別する識別情報としてID、パスワード等を用い情報保管装置30が、情報保管装置30に登録されている識別情報とを照合するようにしてもよい。

図11に、共有メンバーAの削除前の暗号化情報の構成と、削除後の構成を示す。ここでは、暗号化情報として、共有メンバーA用の暗号化共通鍵Aがもとの暗号化情報から削除されていることを示している。

【0066】

次に本実施形態の暗号化復号化装置10の動作を具体例をあげて詳細に説明す

る。

まず第1の実施例として、ユーザBが、チーム101（ユーザA、B、Cの3人が所属）で共有しているスケジュールの1998年の10月1日の項目に用件「セミナー参加」と「15:00」を加える際の処理を説明する。なお本実施例では、スケジュールに関する情報は暗号化情報と暗号化されていない情報を含み、外部の情報保管装置30に保管されているものとする。また情報保管装置30は、ユーザのアクセス権に応じて保管されている情報に対するアクセスを制限できるものとする。また、ユーザBが使用する暗号化復号化装置10は、ユーザBによるデータの入力を受け付ける入力部（図示せず）と、情報を表示する表示部（図示せず）を備えているものとする。

【0067】

まず、ユーザBは暗号化復号化装置10から情報保管装置30にアクセスし、チーム101の1998年10月のスケジュールにアクセスできるか確認する。

【0068】

アクセス可能である場合、チーム101の1998年10月のスケジュールにアクセスする。情報保管装置30は、チーム101の1998年10月のスケジュールを暗号化復号化装置10に転送し、暗号化復号化装置10はその表示部にスケジュールを表示する。なお、この段階ではスケジュールの情報はまだ暗号化されていないものとする。

【0069】

ユーザBは、暗号化復号化装置10の入力部を用いて1998年の10月1日の項目に「セミナー参加」と「15:00～」を入力する。

【0070】

次に、共通鍵暗号化部16において共通鍵を生成する。本実施例ではこの共通鍵をcKey1と呼ぶことにする。

【0071】

次に、共通鍵暗号化部16で、ユーザA、ユーザB、ユーザCの公開鍵を利用して、例えば公開鍵暗号方式であるRSA方式で暗号化する。こうして共通鍵暗号化部では、3人のユーザに対応して3つの暗号化共通鍵が生成される。本実施

例ではこれらの暗号化共通鍵をそれぞれ、eKey1A、eKey1B、eKey1Cと呼ぶことにする。

【0072】

次に、共通鍵改竄検出情報作成部17は、共通鍵のメッセージダイジェストであるMDを作成し、さらにこのMDにユーザBの秘密鍵を利用して署名を行なう。この署名を行なったMDが鍵情報であるSignedKey1である。

【0073】

データ暗号化部21は、スケジュールのデータパーツである「セミナー参加」を共通鍵cKey1で暗号化を行ない、暗号文CryptData1を生成する。

【0074】

次に、データ改竄検出情報作成部22は、一例としてハッシュ関数であるMD5を利用して「セミナー参加」のメッセージダイジェストMessageD1を生成する。

【0075】

「セミナー参加」に適用した手順をスケジュールのデータパーツである「15:00～」に対して行ない、「15:00～」の暗号文CryptData2とメッセージダイジェストMessageD2を得る。

【0076】

そしてこれらの情報を暗号化復号化装置10から情報保管装置30に転送する。

なお、このときの情報保管装置30に記憶される情報の構成を図12に示す。上記処理で作成されたスケジュールを区別する情報、ユーザIDと暗号化共通鍵、鍵情報、暗号文とデータ改竄検出情報および関連情報が記憶される。

【0077】

次に第2の実施例として、第1の実施例からさらに、第1の実施例で作成された暗号化情報にユーザAが、チーム101（ユーザA、B、Cの3人が所属）で共有しているスケジュールの1998年の10月2日の項目に用件「会議」と「17:00～」を加える際の処理を説明する。



【0078】

まず、ユーザAは暗号化復号化装置10から情報保管装置30にアクセスし、チーム101の1998年10月のスケジュールにアクセスできるか確認する。

【0079】

アクセス可能である場合、チーム101の1998年10月のスケジュールにアクセスする。情報保管装置30は、暗号化共通鍵eKey1Aと鍵情報SignedKey1を暗号化復号化装置10に転送する。

【0080】

ユーザAは、暗号化復号化装置10の入力部を用いて1998年の10月2日の用件項目に「会議」と「17:00～」を入力する。

【0081】

次に、共通鍵復号化部18は、ユーザAの秘密鍵を用いて暗号化共通鍵eKey1Aを復号化し共通鍵cKey1を生成する。

【0082】

次に、共通鍵改竄検出情報作成部19は、共通鍵cKey1のメッセージダイジェストkeyD1'を作成する。

【0083】

次に、改竄検証部20は、鍵情報のSignedKey1をユーザBの公開鍵を利用して復号化し、暗号化前の共通鍵のメッセージダイジェストkeyD1を得る。そして、keyD1とkeyD1'を比較する。keyD1とkeyD1'が等しければ、チーム101に所属するユーザBによって作成された共通鍵を改竄されることなく取得できたことがわかる。こうして共通鍵の正当性が確認できる。ここで、ユーザBが共通鍵を作成することが正当であるかどうか、すなわち、共通鍵作成者自身の正当性確認は、共通鍵作成者正当性確認用情報として取得する必要がある。この場合の共通鍵作成者正当性確認用情報の取得方法の一例としては、共通鍵作成者がユーザBであることを暗号化復号化装置10の表示部にダイアログボックスとして表示し、ユーザに確認してもらう方法をとってもよい。または、ネットワークを介して情報保管装置30から関連情報として取得してもよい。

【0084】

次に、データ暗号化部21は、スケジュールのデータパーツである「会議」を共通鍵cKey1で暗号化を行ない、暗号文CryptData3を生成する。

【0085】

次に、データ改竄検出情報作成部22は、一例としてハッシュ関数であるMD5を利用して「会議」のメッセージダイジェストMessageD3を生成する。

【0086】

「会議」に適用した手順をスケジュールのデータパーツである「17:00～」に対して行ない、「17:00～」の暗号文CryptData4とメッセージダイジェストMessageD4を得る。

【0087】

そしてこれらの情報を暗号化復号化装置10から情報保管装置30に転送する。

なお、このときの情報保管装置30に記憶される情報の構成を図13に示す。上記処理で暗号文とデータ改竄検出情報が追加されているところを示している。

【0088】

次に第3の実施例として、第1、第2の実施例で作成され情報保管装置30に保管されているチーム101の1998年10月のスケジュールをユーザCが参照する場合の処理を説明する。

【0089】

まず、ユーザCは暗号化復号化装置10から情報保管装置30にアクセスし、チーム101の1998年10月のスケジュールにアクセスできるか確認する。

【0090】

アクセス可能である場合、チーム101の1998年10月のスケジュールにアクセスする。情報保管装置30は、チーム101の1998年10月のスケジュールと暗号化共通鍵eKey1Cと鍵情報SignedKey1を暗号化復号化装置に転送する。

【0091】

共通鍵復号化部18は、ユーザCの秘密鍵を用いて暗号化共通鍵eKey1Cを復号化し共通鍵cKey1を得る。

【0092】

次に、共通鍵改竄検出情報作成部19で、共通鍵cKey1のメッセージダイジェストcKeyD'を作成する。

【0093】

改竄検証部20では、SignedKey1をBの公開鍵を用いて復号化し、暗号化前の共通鍵のメッセージダイジェストcKeyDを得る。そして、このメッセージダイジェストcKeyDと先のメッセージダイジェストcKeyD'を比較する。この2つのメッセージダイジェストが等しければチーム101に所属するユーザBによって作成された共通鍵cKey1を改竄されることなく取得できたことが検証できる。すなわち、取得した共通鍵の正当性を確認することができる。また、ここで共通鍵作成者自身の正当性確認を行なう必要があるが、第2の実施例で説明したとうりである。

【0094】

次に、データ復号化部23は、暗号文CryptData1を共通鍵復号化部18より取得した共通鍵cKey1を用いて復号化を行なう。ここで平文「セミナー参加」が得られる。

【0095】

次に、データ改竄検出情報作成部24で、ハッシュ関数の1つであるMD5を用いて平文のメッセージダイジェストMessageD1'を生成する。

【0096】

情報保管装置30より転送されてきたメッセージダイジェストMessageD1とデータ改竄検出情報作成部24で生成されたメッセージダイジェストMessageD1'を比較する。これら2つのメッセージダイジェストが等しければチーム101に所属する者によって作成されたデータパーツを改竄されることなく取得できたことがわかる。

【0097】

同様の手順を繰り返すことで暗号文CryptData2…CryptData

a4に対して行なうと、「15:00～」、「会議」、「17:00～」を得ることができる。復号化後のスケジュールの表示例を図14に示す。図に示すようにユーザBが入力したデータパーツ「セミナー参加」、「15:00～」とユーザAが入力したデータパーツ「会議」、「17:00～」を同じチームに所属するユーザCは見ることができる。

## 【0098】

以上のように、1つのチームに所属する共有メンバーは、暗号化情報に対するデータパーツの追加や変更、他共有メンバーのデータパーツの参照等、自由に行なえるが、共有メンバー以外の者に対して秘匿性を保つことができる。

## 【0099】

また一例として、MessageD1、…、MessageD4の各サイズを16バイト、鍵情報のサイズを2300バイト（下限がある）であるとする、本実施例では

$$16 \times 4 + 2300 = 2364 \text{ バイト}$$

がオーバーヘッドとなる。

従来の方式で4つの暗号文のそれぞれに署名を付ける場合は

$$2300 \times 4 = 9200 \text{ バイト}$$

のオーバーヘッドとなり、本発明の方式が従来方式より情報量を抑えることができる。

## 【0100】

なお、本発明は、インターネットの他、LANやダイヤルアップによるネットワークを利用してもよい。

また、本発明の暗号化装置、復号化装置、及び方法を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号化、復号化の処理を行ってもよい。

すなわち、暗号化プログラムを記録したコンピュータ読み取り可能な記録媒体において、暗号化プログラムは、共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する機能と、公開鍵暗号方式を利用して前記共通鍵を暗号化

し暗号化共通鍵とする機能と、前記共通鍵より鍵情報を作成する機能と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする機能と、前記平文より第1データ改竄検出情報を作成する機能をコンピュータに実現させる。

また、復号化プログラムを記録したコンピュータ読み取り可能な記録媒体において、復号化プログラムは、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する機能と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する機能と、前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する機能と、前記暗号文を共通鍵暗号方式で復号化する機能と、前記暗号文を復号化した平文より第2データ改竄検出情報を作成する機能と、前記第1データ改竄検出情報と前記第2データ改竄検出情報とから改竄検証する機能をコンピュータに実現させる。

#### 【0101】

なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピーディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

#### 【0102】

以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

#### 【0103】

【発明の効果】

以上、詳細に説明したように、本発明によれば平文毎に改竄検出情報を作成することはせず、各平文を暗号化する共通鍵に対して改竄検出情報となる鍵情報を作成し、改竄検出と共通鍵作成者の本人確認を可能としたので、情報を暗号化した暗号化情報のオーバーヘッドを減少させることができる。したがって、暗号化情報の転送時におけるネットワークにかかる負荷と暗号化情報を保管する際に要する記憶装置の容量を減少させることができる。また、各平文に第1データ改竄検出情報を付加したので、個々の平文毎に改竄検出が可能である。また、利用者毎に暗号化共通鍵を作成することで複数の利用者間で暗号化情報を共有できる。

【図面の簡単な説明】

【図1】 本発明の一実施形態である暗号化復号化装置の構成を示すブロック図である。

【図2】 本発明の一利用形態を示す図である。

【図3】 暗号化に係る動作を説明するフローチャートである。

【図4】 暗号化前の情報と暗号化情報の構成を示す図である。

【図5】 復号化に係る動作を説明するフローチャートである。

【図6】 暗号化情報に情報を追加する際の動作を説明するフローチャートである。

【図7】 暗号化情報に情報を追加する前後の暗号化情報の構成を示す図である。

【図8】 共有メンバーBが、チームに共有メンバーCを追加する際の動作を説明するフローチャートである。

【図9】 チームに共有メンバーCを追加する前後の暗号化情報の構成を示す図である。

【図10】 チームから共有メンバーを削除する際の動作を説明するフローチャートである。

【図11】 チームから共有メンバーAを削除する前後の暗号化情報の構成を示す図である。

【図12】 第1の実施例における情報保管装置に記憶されている情報を示

す図である。

【図 13】 第 2 の実施例において情報を追加した際の情報保管装置に記憶されている情報を示す図である。

【図 14】 第 3 の実施例において復号化後のスケジュールの表示例を示す図である。

【図 15】 従来の暗号化・署名方式における暗号化の動作を説明するフローチャートである。

【図 16】 従来の暗号化・署名方式における復号化の動作を説明するフローチャートである。

【図 17】 特開平 8-156964 に開示されている暗号化方式による暗号化前の情報と暗号化情報の構成を示す図である。

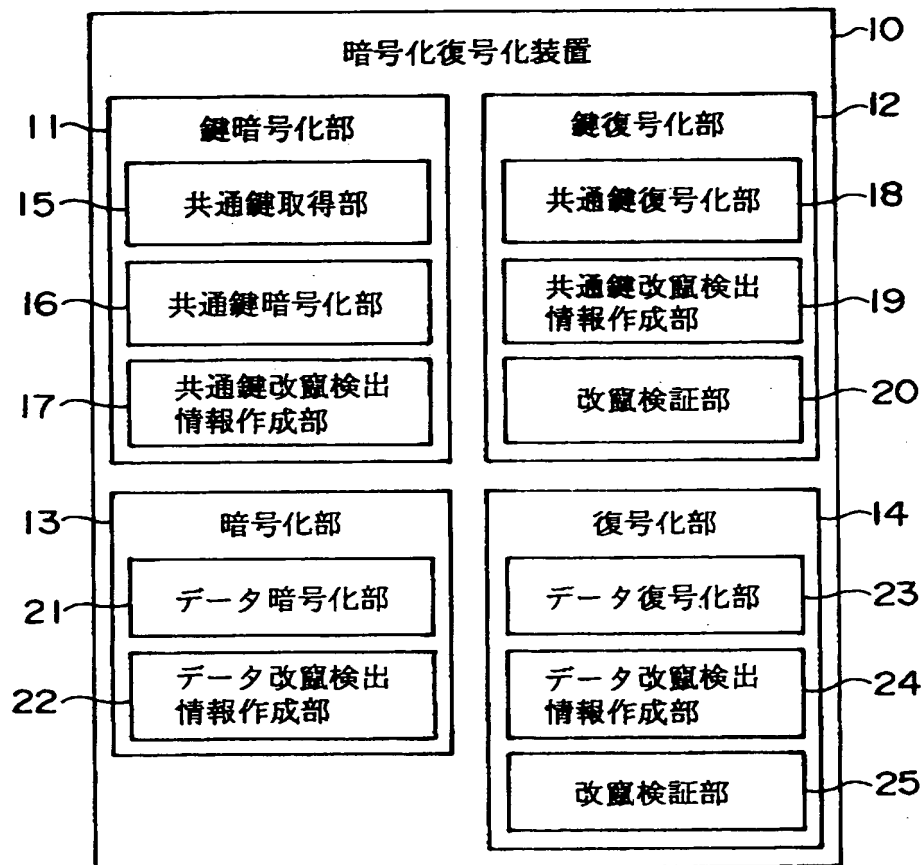
【図 18】 特開平 9-71388 に開示されている暗号化方式による暗号化前の情報と暗号化情報の構成を示す図である。

【符号の説明】

10…暗号化復号化装置	11…鍵暗号化部
12…鍵復号化部	13…暗号化部
14…復号化部	15…共通鍵取得部
16…共通鍵暗号化部	17…共通鍵改竄検出情報作成部
18…共通鍵復号化部	19…共通鍵改竄検出情報作成部
20…改竄検証部	21…データ暗号化部
22…データ改竄検出情報作成部	23…データ復号化部
24…データ改竄検出情報作成部	25…改竄検証部
30…情報保管装置	31…端末装置

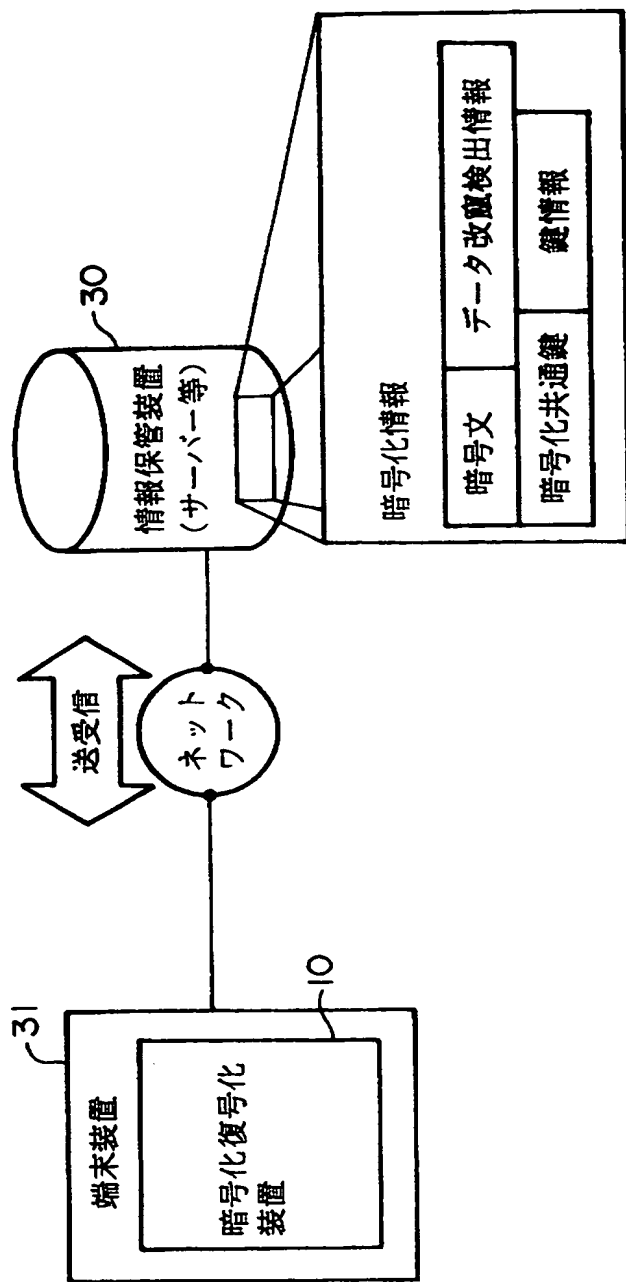
【書類名】 図面

【図 1】

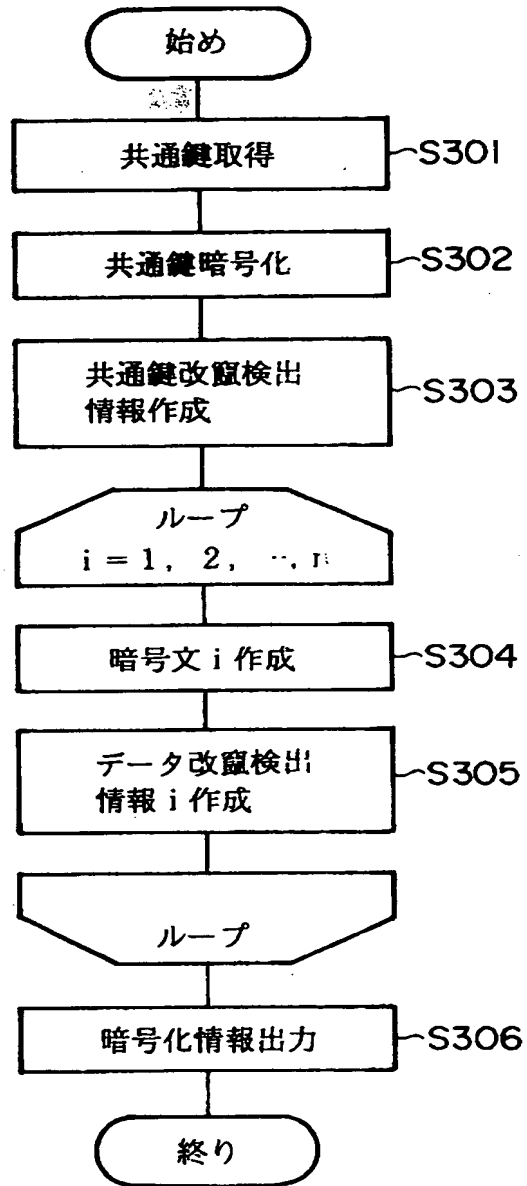




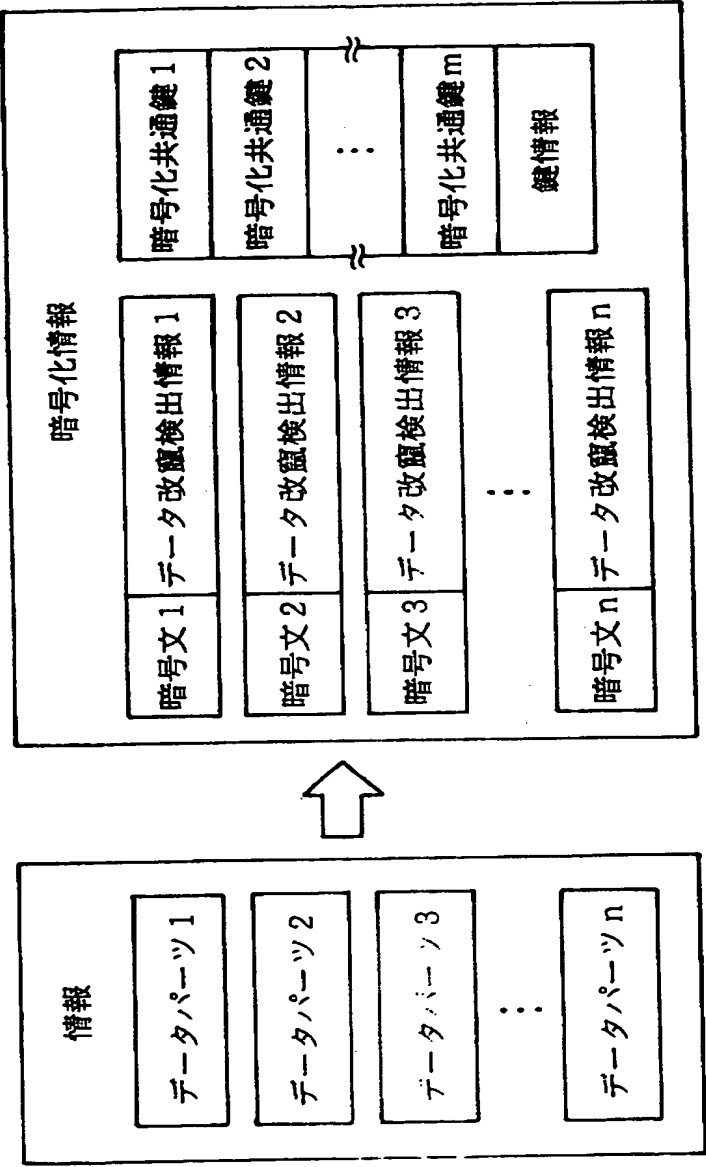
【図2】



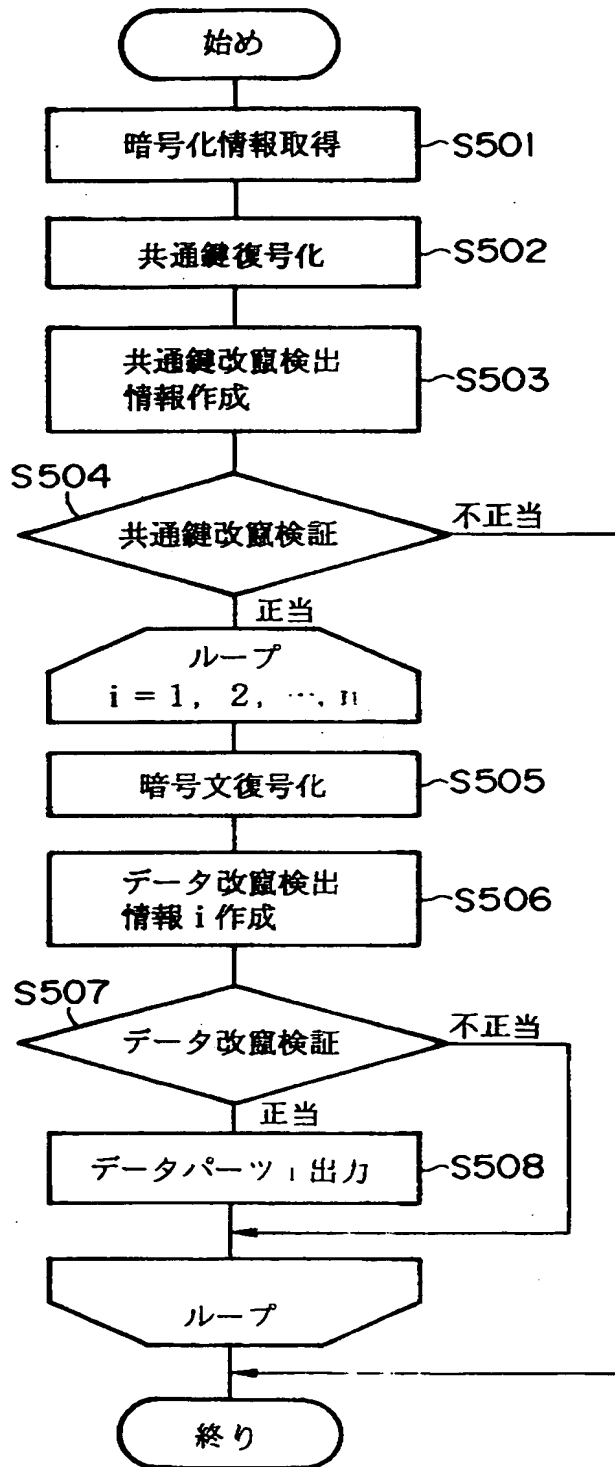
【図 3】



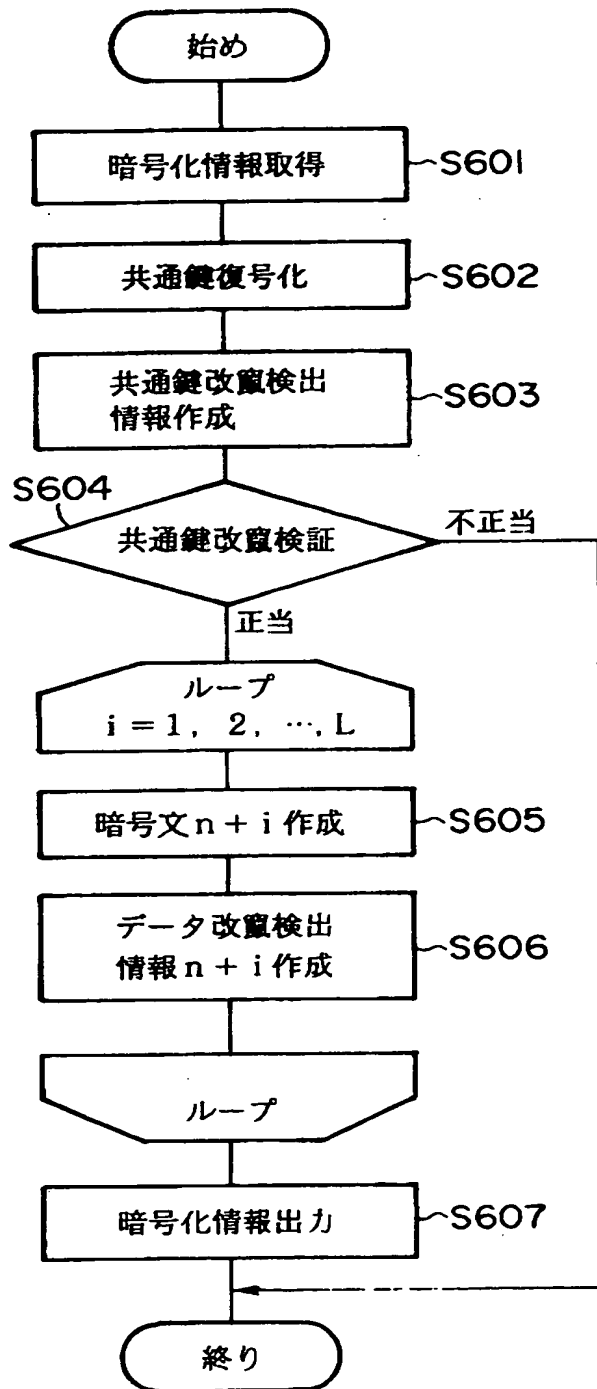
【図 4】



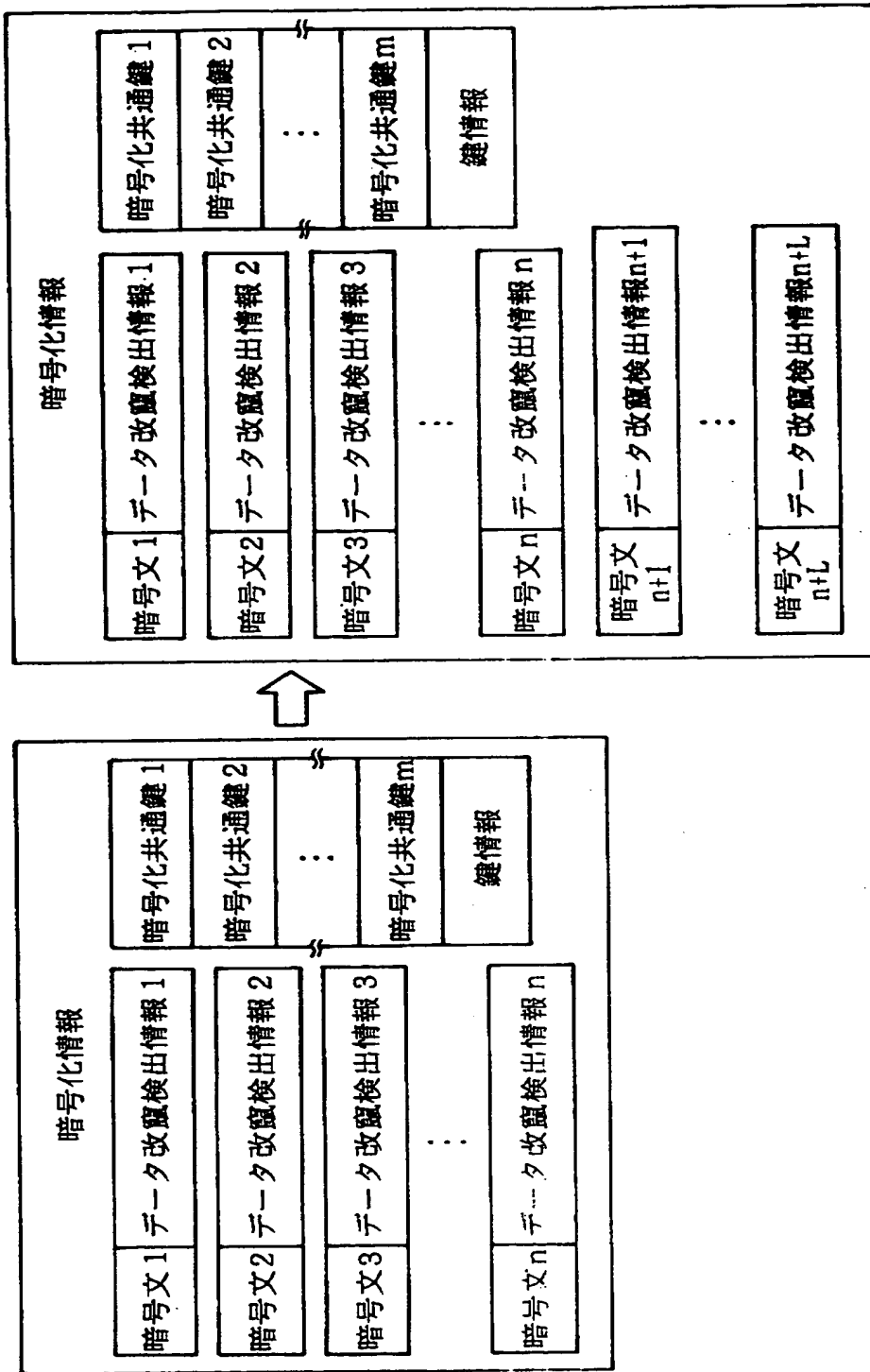
【図5】



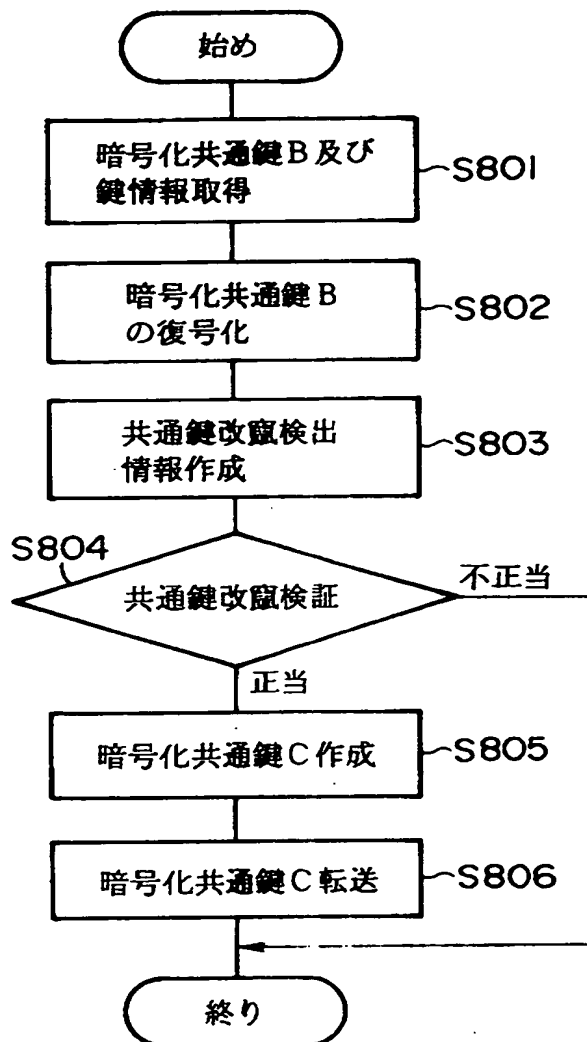
【図 6】



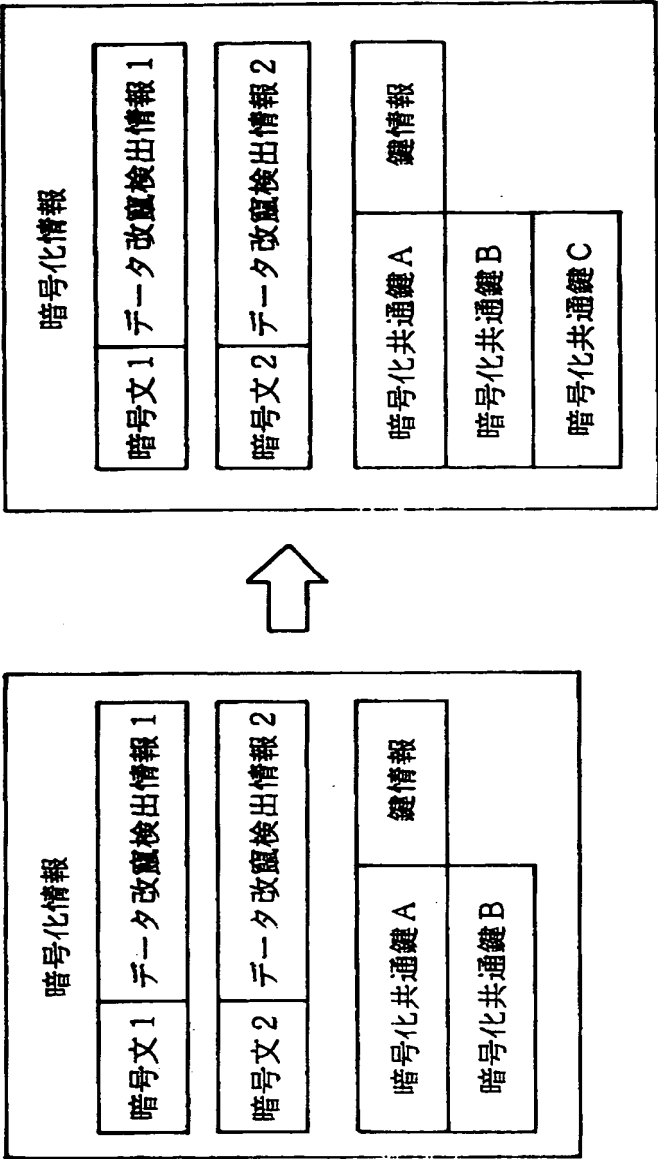
【図 7】



【図 8】

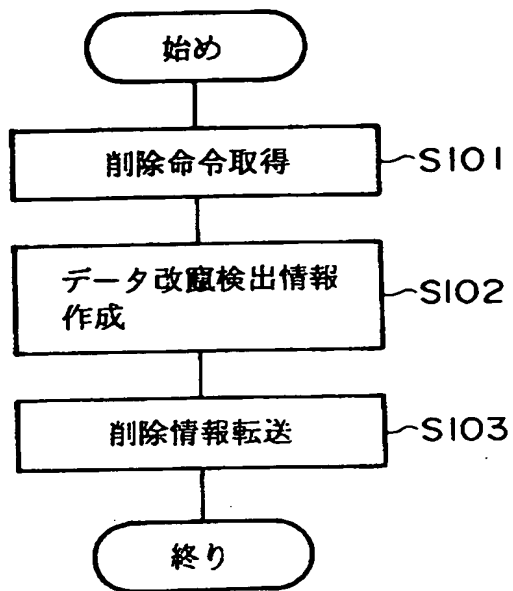


【図9】

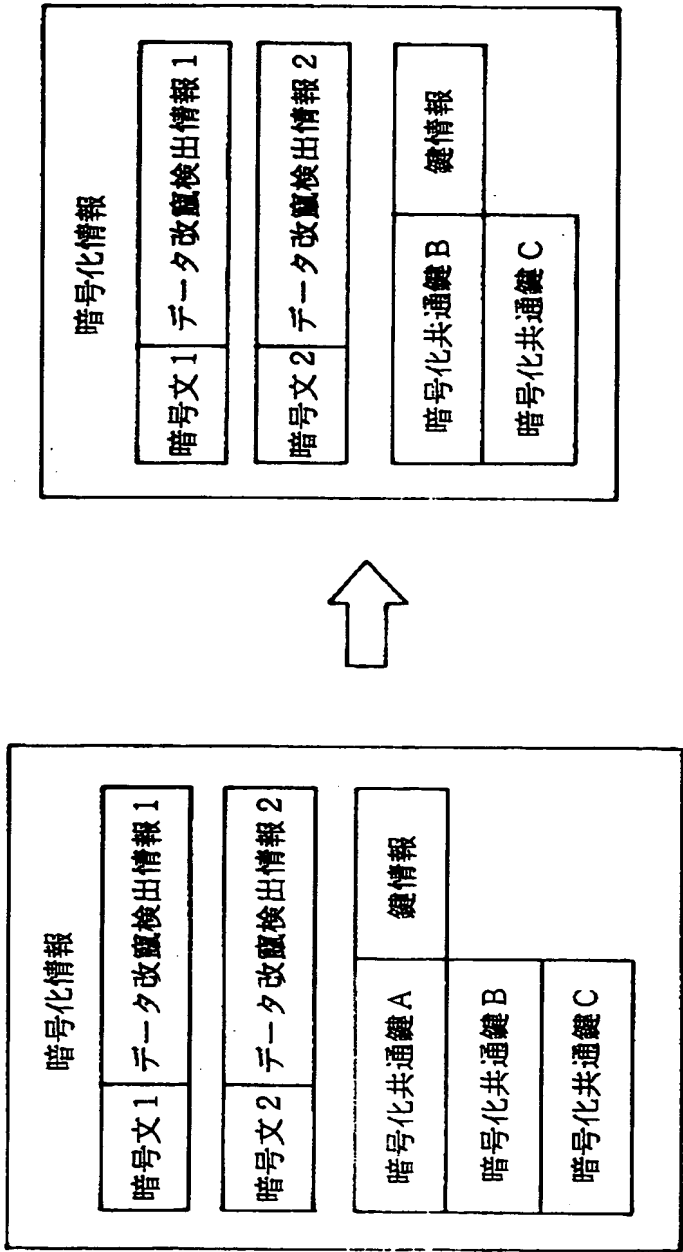




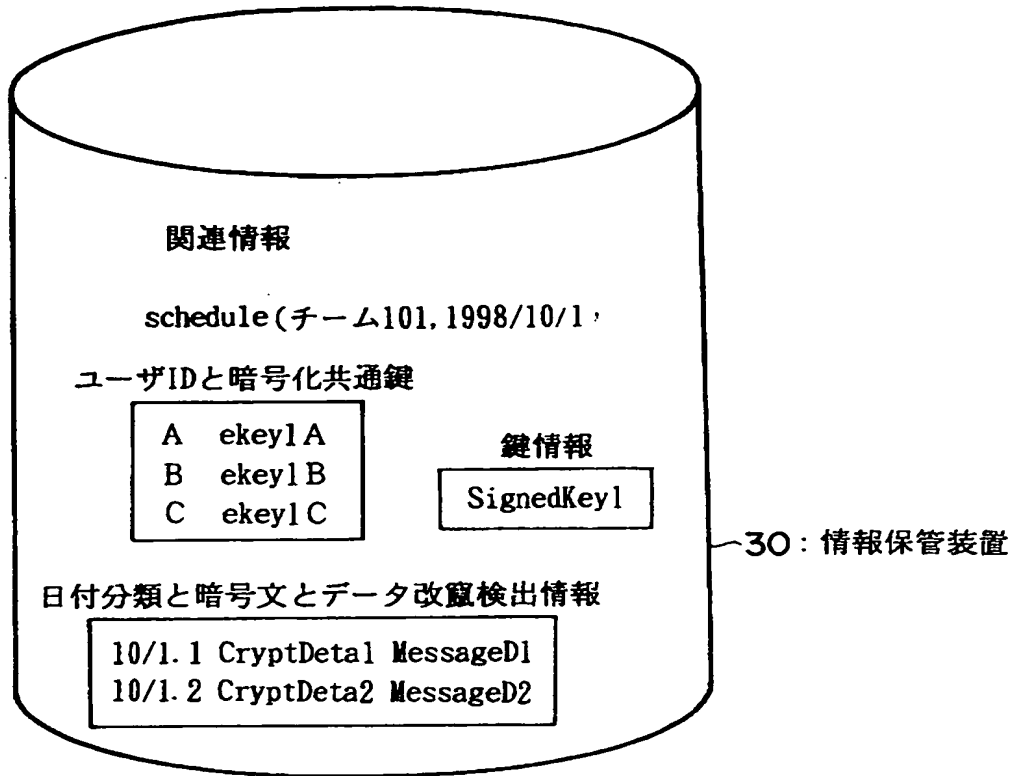
【図 10】



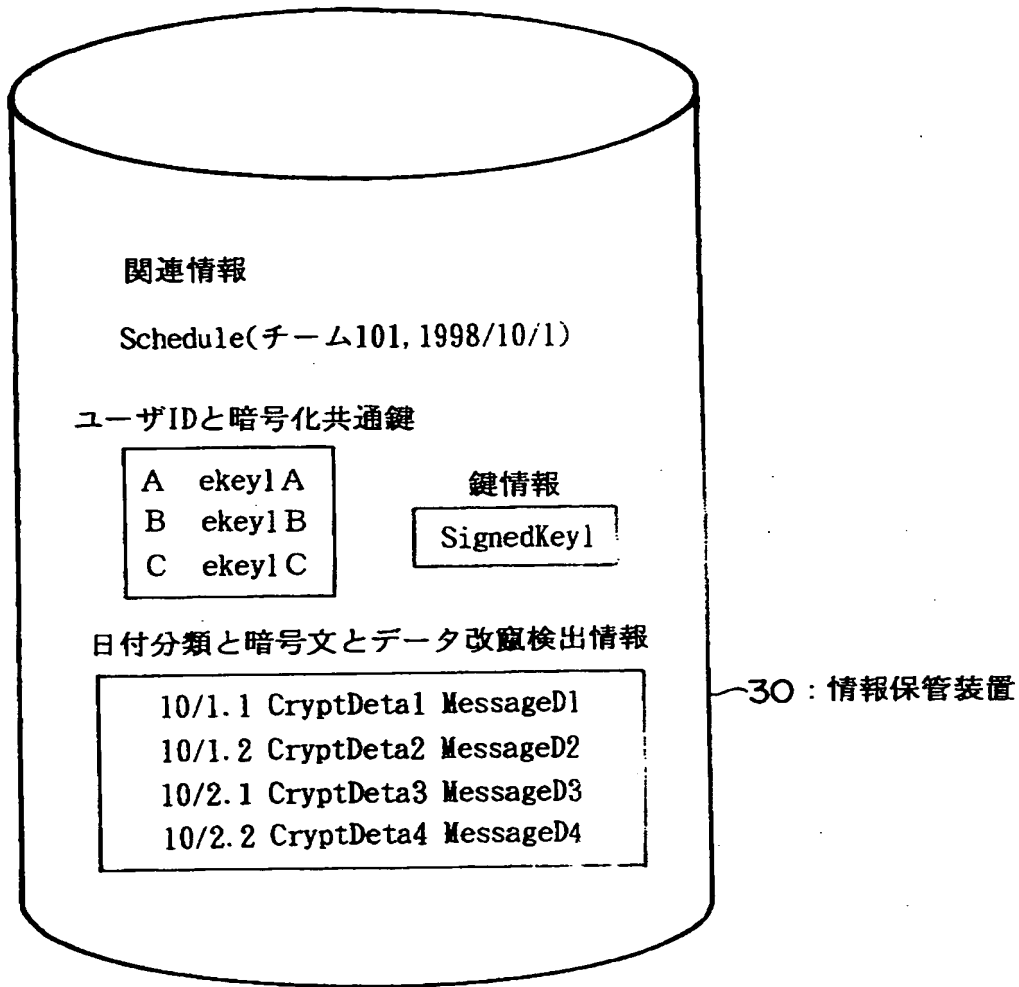
【図11】



【図 12】



【図13】



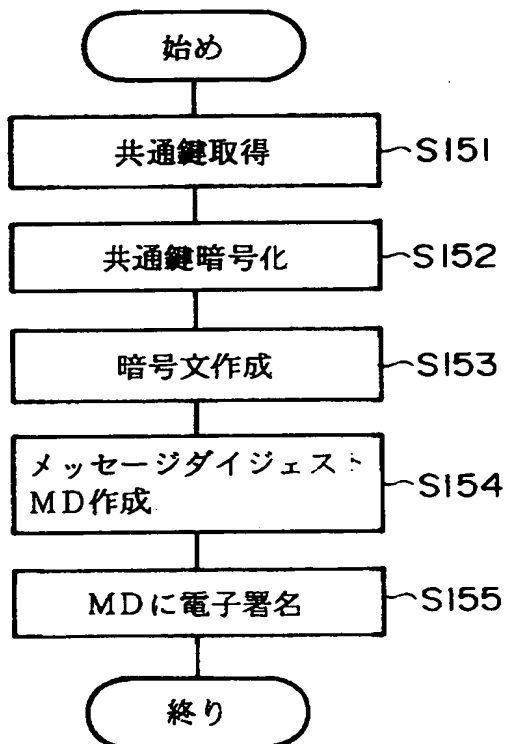
【図14】

チーム101：スケジュール

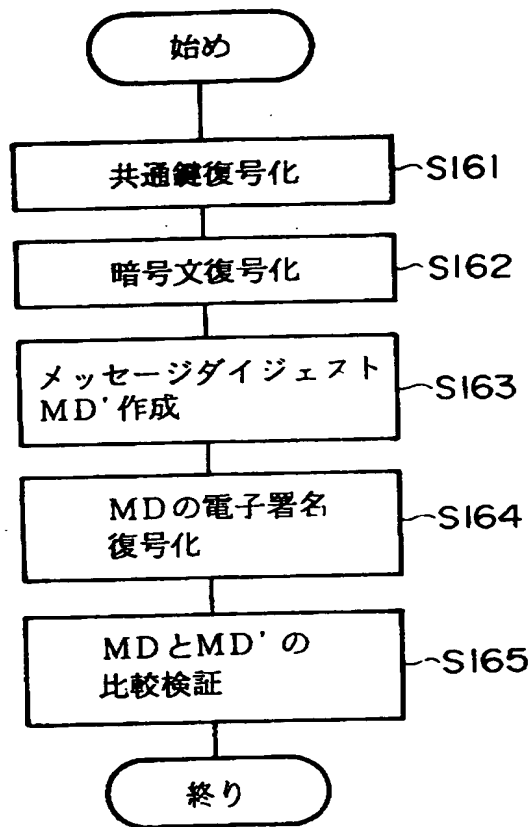
10月

1日 B：セミナー参加 15:00～	2日 A：会議 17:00～	

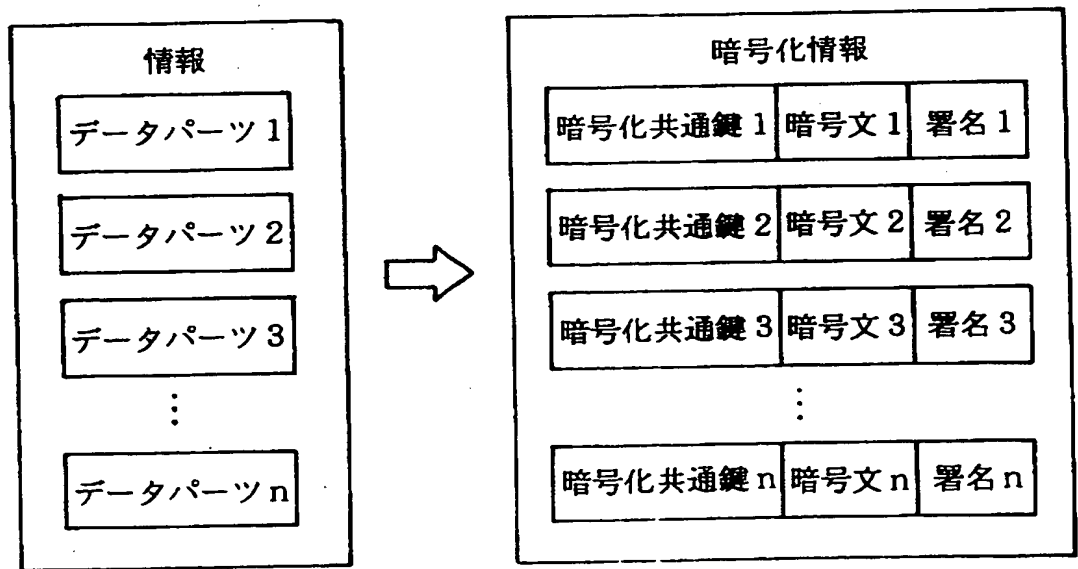
【図15】



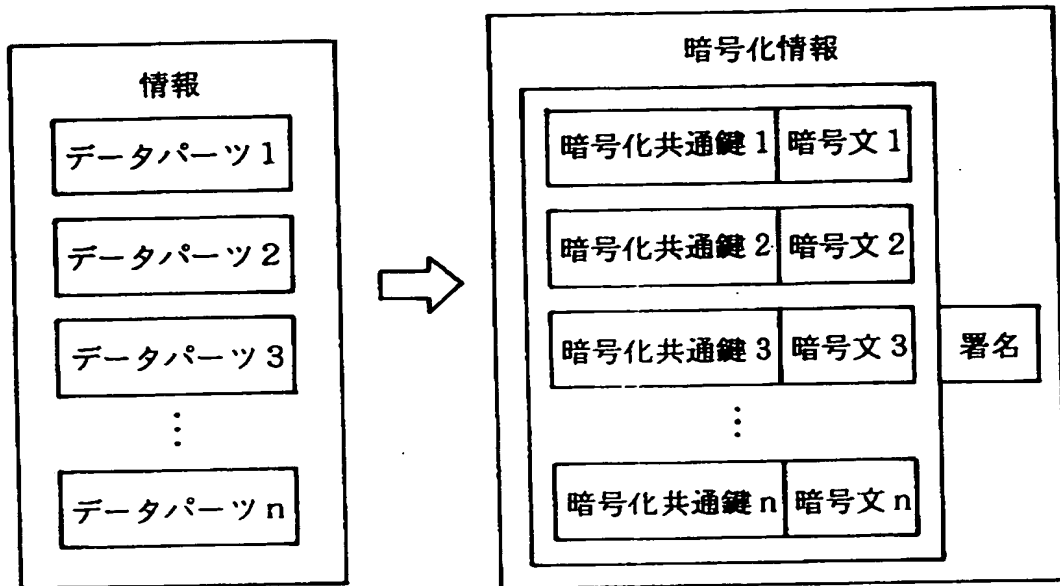
【図 16】



【図 17】



【図 18】



【書類名】 要約書

【要約】

【課題】 複数の共有メンバーからなるチームで暗号化情報を共有可能とし、暗号化情報自体のオーバーヘッドが少なく、また改竄検証を可能とする暗号化復号化装置を提供する。

【解決手段】 本発明の暗号化復号化装置は、暗号化に際し、平文の暗号化・復号化に共通鍵方式を用い、各暗号文ごとに第1改竄検出情報を作成し、共通鍵を共有メンバー毎の公開鍵で暗号化するとともに共通鍵の改竄を検出するための鍵情報を1つのみ作成する。また復号化に際しては、復号化した共通鍵から共通鍵改竄検出情報を作成し、鍵情報と比較し共通鍵の改竄を検証する。また復号化した平文から第2改竄検出情報を作成し、第1改竄検出情報と比較し平文の改竄を検証する。

【選択図】 図1



【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000006264  
【住所又は居所】 東京都千代田区大手町1丁目5番1号  
【氏名又は名称】 三菱マテリアル株式会社

【代理人】

申請人

【識別番号】 100064908  
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル  
志賀国際特許事務所

【氏名又は名称】 志賀 正武

【選任した代理人】

【識別番号】 100108578  
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル  
志賀国際特許事務所

【氏名又は名称】 高橋 詔男

【選任した代理人】

【識別番号】 100089037  
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル  
志賀国際特許事務所

【氏名又は名称】 渡邊 隆

【選任した代理人】

【識別番号】 100101465  
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル  
志賀国際特許事務所

【氏名又は名称】 青山 正和

【選任した代理人】

【識別番号】 100094400  
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル  
志賀国際特許事務所

【氏名又は名称】 鈴木 三義

【選任した代理人】

【識別番号】 100106493  
【住所又は居所】 東京都新宿区高田馬場3丁目23番3号 ORビル  
志賀国際特許事務所

【氏名又は名称】 松富 豊

【選任した代理人】

【識別番号】	100107836
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	西 和哉
【選任した代理人】	
【識別番号】	100108394
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	今村 健一
【選任した代理人】	
【識別番号】	100108453
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	村山 靖彦
【選任した代理人】	
【識別番号】	100100077
【住所又は居所】	東京都新宿区高田馬場3丁目23番3号 ORビル 志賀国際特許事務所
【氏名又は名称】	大場 充

出 願 人 履 歴 情 報

識別番号 [000006264]

1. 変更年月日 1992年 4月10日  
[変更理由] 住所変更  
住 所 東京都千代田区大手町1丁目5番1号  
氏 名 三菱マテリアル株式会社

***This Page Blank (uspto)***

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

This Page Blank (uspto)